CryptoLocker „zsaroló-vírus”

Az alábbi cikk elsődlegesen a CryptoLocker kártevő-program működését ismerteti és a fertőzés elleni védekezést próbálja meg segíteni, de hasznos a többi, nem ennyire drasztikus eredményt produkáló számítógépes kártevőprogram elleni védekezésben is.

A CryptoLocker működésének bemutatása

A **CryptoLocker ransomware** első detektálása 2013 szeptemberében történt. A **Microsoft operációs rendszer**ű (Windows XP, 7, 8, 8.1) számítógépes rendszerekben **tud kárt tenni**, a többi platform (Apple, Linux, stb...) nem veszélyeztetett. Az áldozat számítógépének meg**fertőzése után a háttérben RSA (un. aszimmetrikus, kétkulcsos) titkosítási algoritmussal**, nyilvános („public key”) kulccsal **titkosítja a számítógépen található „személyes fájlokat”** (Word, Excel, PowerPoint, kép és videó-fájlokat, stb…). Végül a ransomware egy **felbukkanó ablakban** (angol nyelven) **tájékoztat a számítógépen található dokumentumok titkosításáról és pénzt követel a helyreállításhoz feltétlenül szükséges egyedi titkos-kulcsért** („private key”)**.** A felbukkanó ablak bal oldalán **megjelenik egy számláló** is**, ami 72 órától visszafelé számol** 0-ig, ami a váltságdíjfizetés határidejének leteltéig hátralévő, **fennmaradó időt mutatja**. A fenyegetés szerint a **72 órás határidő letelte után törlik a szerverükről** a titkosított „személyes fájlok” helyreállításához szükséges egyedi **„private key”-t** és ezzel az érintett **adatok örökre elvesznek**. CryptoLocker verziótól függően a **fizetendő „váltságdíj” 0,5-2 bitcoin, vagy 100-300 USD, vagy EUR összeg**. Sajnos a **jelenlegi informatikai technikával** ez a 2048/4096bites RSA titkosítás (katonai/banki „erősségű”) **nem törhető fel**, így **akinek pótolhatatlan adatait érintette a fertőzés** és **szeretné helyreállítani** azokat, az kénytelen **kifizetni a „váltságdíjat”** és **bízni abban, hogy ezután a zsarolók elküldik a dekódoláshoz szükséges egyedi, titkos-kulcsot**. Internetes honlapok szerint az USA rendőrsége is kénytelen volt fizetni több száz USD váltságdíjat, mert nem volt naprakész mentésük a dokumentumaikról (link). Előfordult, hogy a rendszergazda gyanútlanul csatlakoztatta a fertőzött számítógéphez az egyetlen adatmentést tartalmazó külső HDD-t és így az azon tárolt adatok is használhatatlanná váltak, mert a CryptoLocker titkosította ezeket a fájlokat is.

Fertőzés forrásai lehetnek:

- **Email:** A CryptoLocker első verziói főleg **spamekhez csatolt .zip-fájlok**ban terjedtek,
- **Weboldalak: „Támadó”-weboldalakról,** torrent, warez oldalakról **fájlok letöltése, futtatása**, **„felnőtt”-tartalmú oldalak meglátogatásakor** (vagy **feltört weboldalakon**) **lefutó támadó kód**, ami a fertőzéshez **kihasználja** az operációs rendszer és/vagy a böngésző-program **biztonsági réseit**.
- **Mobil adattároló eszközök**: **Fertőzött pendrive**, memóriakártya, külső merevlemez, stb...

Megelőzés

- **Rendszeresen készítsen mentést** a fontos, pótolhatatlan dokumentumairól, ha lehetséges több egymástól független adattároló eszközre is (pl. csak egyszer írható DVD, pendrive, külső HDD, stb…)! **Menteni, menteni, menteni, ez a legfontosabb!!** Végül amennyiben lehetséges **az adattároló eszközt átkapcsolni csak olvasható (read only) állapotba.**
- Telepítsen **hatékony antivírus szoftver**t és **frissítse** naponta az adatbázisát!
- Windows **operációs rendszer legyen** mindig **naprakész**, **Windows Update** legyen **automatikus letöltés**re, **telepítés**re állítva.
- A 2014. április óta már nem támogatott **Windows XP helyett** (amennyiben a hardver erre megfelelő) telepítsen frissebb, még **támogatott operációs rendszer**t!
- **Minden** más **alkalmazás** is **legyen naprakész** (pl. Office programcsomag, Adobe Reader és Flash, Java, böngészőprogramok: Chrome, Firefox, Internet Explorer, stb…), legyen letöltve, telepítve a legfrissebb verzió, patch, amelyekben javítva vannak az időközben felfedezett, javított sérülékenységek. A régebbi szoftververziókban található sebezhetőséget kihasználva könnyen megfertőzhetik a számítógépet a kártevőprogramok (nem csak a CryptoLocker).
- **Korlátozott jogosultságú felhasználói fiókot használjon** a szokásos napi munkák végzéséhez rendszergazdai jogosultságú fiók helyett.
- **Ismeretlen feladótól**, **gyanús tartalmú e-mail**ekben érkező (zip) **csatolmányokat nem** szabad **megnyitni**.
- Warez és más „gyanús”, **nem megbízható weboldalakat nem** kellene **látogatni**, illetve **használjon „webfilter”-t**.
- **Legyen óvatos, amikor egy weboldal plug-in telepítését javasolja**!
- **Senkinek ne adja ki személyes adatait!** (pl. jelszó, banki adatok stb…)
- **Legyen gyanakvó a szokatlan, gyanús eseményekkel szemben!**
- **Hordozható adattároló eszközökön** (pl. pendrive) található **fájlokat** csak **vírusellenőrzés után nyissuk meg**.
- **Ne legyen indokolatlanul csatlakoztatva** a **hordozható adattároló eszköz** a számítógéphez! Lehetőleg **csak mentéskor**, illetve **adat-visszaállításkor**.

„Katasztrófa” elhárítás

- Amennyiben **NINCS naprakész mentés** a pótolhatatlan „**személyes fájlokról**” és **szeretné újra olvashatóvá tenni**:
  - Sajnos **ki kell fizetni a „váltságdíjat”** a titkos kulcsért, amilyen hamar csak lehet és kövesse a fájlvisszaállításhoz a megadott lépéseket.
- Amennyiben **VAN naprakész mentés**:
  - **Távolítsa el a CryptoLockert egy hatékony vírusirtó szoftverrel**, **vagy**
  - **Telepítse újra az operációs rendszert**.
  - **Állítsa vissza a személyes fájlokat a mentésből**.

Weboldalak a témával kapcsolatban:

en.wikipedia.org/wiki/CryptoLocker
www.hwsw.hu/hirek/51349/cryptolocker-virus-ransomware-malware-symantec.html
sg.hu/cikkek/103893/titkositja-adatainkat-a-cryptolocker-virus
www.theguardian.com/money/2014/feb/27/pc-users-beware-cryptolocker-malware-royal-mail
blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/
www.welivesecurity.com/2013/12/19/cryptolocker-2-0-new-version-or-copycat/
http://www.theguardian.com/technology/2013/nov/21/us-police-force-pay-bitcoin-ransom-in-cryptolocker-malware-scam
http://thehackernews.com/2013/11/us-police-department-pays-750-ransom-to.html

Készítette:
Ludman Tamás
mérnök informatikus
tamas@ludman.hu
www.ludman.hu

Budapest, 2015. január 21.